FINTECH FUTURES | REPORTS

ISACA

# Rising threats and new challenges: the changing face of cybersecurity

# Introduction

The financial services sector, while traditionally one of the more secure industries in the world from a security and resiliency perspective, has had to face several challenges in the past two years or so. These have tested the sector's ability to rise to new challenges, adapt to changing circumstances, and rapidly accelerate digital processes in reaction to customer and employee demands.

While the banking sector has faced the risk of cyberattack for many decades – and has built standardised defences to prevent major breaches – many of these legacy strategies and processes struggle to meet the needs of a rapidly changing world.

Even the best of walls can be flown over or dug underneath, and defence in depth against traditional attack vectors is no use when having to open up to millions of new touchpoints in the wake of the COVID-19 pandemic.

Every weakness can be exploited by a cybercriminal organisation or a bad state actor. Bad actors have utilised this disruption, with a rise of 238% in cyberattacks targeting financial institutions since the start of the pandemic,[1] part of an even wider surge of 1,318% in ransomware attacks across all sectors in the first half of 2020.[2]

Yet it's not just the bad guys causing issues. New technological trends such as open banking, embedded finance, and hybrid cloud environments are causing massive change in systems, processes, and strategies. A rapid generational shift in technology also opens up avenues for exploitation as organisations fail to protect gaps in their defence networks.

**In 2020...**

**1,318%**
rise in ransomware attacks

**238%**
rise in cyberattacks targeting banks

## Digital changes and new threats

The exponential growth of data has created a new raft of potential security issues. A drive to digital has also created an explosion in customer touchpoints, integrations with partners, and a network of partners and suppliers. The chain has become a web, and just one strand of the web needs to fail for a data breach to work its way inside an institution.

While a movement towards digital systems and channels was well underway prior to 2020, the COVID-19 pandemic has catalysed an explosion in usage. During the pandemic, usage of mobile-based financial apps rose by 72% in just one week.[3]

---

1 https://www.vmware.com/resources/security/modern-bank-heists-2020.html

2 https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup

3 https://ec.europa.eu/commission/commissioners/2019-2024/dombrovskis/announcements/speech-executive-vice-president-valdis-dombrovskis-digital-finance-outreach-2020-closing-conference_en

The march towards greater cloud adoption is well underway: 94% of enterprises use a public cloud in some form or another, while 66% have a central team dedicated to the development of cloud-based technologies.[4]

Despite that, reticence from regulators over the adoption of cloud remains. Previous concerns over data residence and control have made way for new cautions on over-reliance on single suppliers. While banks are shifting applications to the cloud, many core and critical functions remain on-premises. When that new shift occurs, market participants must be ready for the risks that accompany it.

Firms must prioritise the discarding and removal of old assets alongside new technology. Old assets contain old data, but it is still data usable against an organisation. Securing new data through encryption and virtual private networks is a useful next step, across internal operations. Removing existing siloes or managing them through new technology is also recommended.

**72%**

rise in financial mobile apps usage

**94%**

of enterprises using public cloud

**66%**

have a dedicated team for cloud development

## Technology and talent

While the largest organisations are the most tempting targets, and face the prospect of defending against daily attacks, smaller institutions are also at risk for different reasons. Smaller banks can deploy fewer resources to tackle cybersecurity issues and are often forced to outsource or even ignore critical processes, increasing the likelihood of gaps in their defences.

The smaller side of the sector is buckling under the strain. Community banks, lending institutions and credit unions in the US have urged Congress to act to protect them.[5] "Issues of cybersecurity and consumer data rights are intertwined," stated representative and consumer protection chair Ed Perlmutter. "This makes cybersecurity critical for all financial institutions, large and small."

Yet as institutions look to increase their investment in new technology with or without jurisdictional support, they risk multiplying potential attack surfaces for cybercriminals and bad actors. This growing risk is compounded by the traditionally siloed approach to cybersecurity. Processes across the business can be disparate, disconnected, and the remnants of projects undertaken by legacy chief information security officers (CISOs).

A knitting together of these disparate systems will become a crucial part of any organisation's forward-looking cybersecurity strategy. Security Orchestration, Automation and Response (SOAR) systems can leverage both human and machine power to define, rank and kick off incident response activities.

[4] https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf

[5] https://www.rollcall.com/2021/11/09/small-banks-facing-greater-cyber-risks-urge-congress-to-act

> *"We've seen that organisations have 50 plus security tools on average within their organisation. Whether they're using AWS, Azure or the IBM Cloud, there are going to be various tool sets moved into an organisation over the years. Many of these tool sets don't work together. Getting that single pane of glass across an organisation, getting a view on everything, is a demand we're seeing significant traction on.*
>
> **Corey Hamilton**, partner, IBM Security Services

Artificial intelligence (AI) has emerged as one of the most popular and sought-after tools in the repertoire of security professionals in the financial services sector. While the explosion of data outlined earlier can pose challenges, through the application of AI it can create solutions.

About 20% of vendors and software providers in the AI space dedicate their platform to risk and cybersecurity.[6] The technology provides automated detection of the main avenues through which cybercriminals, fraudsters, and others attempt to game the system. Two major solutions are anomaly detection and natural language processing (NLP).

The former focuses on training a model to recognise the behaviour patterns of a group of accounts or users. Then, when one of that group begins to act differently it can be focused upon for greater analysis by a trained specialist.

NLP actions the analysis and identification of anomalies in communications between an organisation and its customers. Trained to recognise when a user's writing patterns have changed, it enables quick sorting through the millions of emails, messages, and other communications banks receive daily from their customers.

Yet it isn't as simple as installing the latest piece of shiny software and calling it a day. Banks are inundated with security alerts on a daily basis: 60% of institutions are facing 100,000 alerts or more every 24 hours, while 37% are hit with more than 200,000.[7]

Identifying the legitimate from the duplicate has become an onerous task, especially as banks deploy more and more tools, and increasing suites of software, to combat new threats emerging daily. Often these tools do not mesh well.

It's a symptom of a software market in which the rapid pace of threat evolution means existing players struggle to reasonably respond to every new threat. Newer entrants and greenfield suppliers are therefore the go-to for banks looking to protect themselves from the latest exploits. In 2017, 73% of financial institutions ran more than 25 tools for their security. That number has no doubt grown.

While technology remains an important bedrock for any seismic change, equal importance needs to be placed on people and process. Talent is becoming harder and harder to find in the market today. There are more than 280,000 openings in cybersecurity today, with predictions the deficit of sector professionals could hit 3.5 million by the end of the year.[8]

Eight in 10 financial services firms report a shortage in cybersecurity skills, and seven in 10 believe this leaves them vulnerable to security breaches. Half of banks say security talent is their most pressing employee shortage.[9]

[6] https://emerj.com/ai-sector-overviews/ai-cybersecurity-in-banking

[7] https://www.americanbanker.com/news/alert-there-are-too-many-cybersecurity-alerts

[8] https://cybersecurityventures.com/jobs

[9] https://www.mcafee.com/uk/resources/reports/rp-hacking-skills-shortage-financial-services-summary.pdf

Companies facing these shortages need to create a talent feedback loop within their organisation – one based on expanding their pool of new employees, developing them with continuous learning, and making retention a priority. New recruits should be capitalised on from day one with progressive and effective onboarding programs.

Cybersecurity is a highly dynamic sector that requires almost continuous learning and upskilling. Providing an effective platform for new starters to hit the ground running can pay immediate dividends. Banks can foster a security and growth network within the organisation by partnering new hires with experienced members of the team. Further, a firm should avoid burning bridges with departing talent, and ensure a reputation in the market as a company to work for, not avoid.

> *"There are plenty of programmes across the globe supplying cybersecurity talent; however, the predominant need is the three to five years of experience group. Organisations must increase the number of entry-level positions to take advantage of feeder programmes. Failure to do so will increase the number of trained people unable to find cybersecurity roles.*

*Focusing on specific tools, methods, or resource experience limits your ability to recruit and retain quality talent. Instead, focusing on key traits, characteristics, and functions of individuals will lead you to quicker development and greater return on investment in your talent management programme.*

**Jon Brandt,** information security professional practices lead, ISACA


# Build cyber resilience

*with ISACA's leading risk-based solution*

74% of financial institutions experienced a rise in cyber crime in the last 12 months. [1]

Cyber attacks can equal up to 233 days of negotiation or downtime for financial institutions. [2]

Firms in the financial industry are 300x more likely to experience a cyber attack. [3]

Mitigate inevitable cyber threats with **ISACA's CMMI Cybermaturity Platform**— the first cybersecurity maturity management platform with evidence-based insights to improve cyber resilience across your organization.

Visit **www.isaca.org/FintechFuturesCybersecurity**

*1 - BAE Systems Applied Intelligence*
*2 - Global Banking and Finance Review*
*3 - Boston Consulting Group*

ISACA Enterprise Solutions

## Embedding security

It's imperative that financial institutions have a strategic, technological, and operational plan in place for how they should defend themselves against threats. Such plans must be in writing, distributed among leaders, and tested frequently against industry standards to ensure readiness.

Installing a lasting and holistic overview of the security function can seem like a herculean challenge for institutions, especially when CISOs have a typically short lifespan at even the largest banks. When undergoing transformation processes that could last a decade or more, it's important to ensure that the ideals and the goals of that change are embedded inside an organisation.

While every CISO will have his favourite toolbox of suppliers and systems, creating a strategy focused on the end goal means a project aimed at strengthening the cybersecurity posture of an institution lasts longer than 18-20 months. Luckily, progress is already being made on this front, with 42% of leaders at financial institutions saying cybersecurity is a crucial part of their agenda and discussed monthly.[10]

> *Ensuring you have a programme that is aligned to an industry recognised framework should be step number one. The second would involve comprehensive programme assessment. Where is the organisation? Where do they want to be in three to five years?*
>
> *Get to a point where you know what will have the highest impact for the least cost. It's not an 'oh this is a red, this is a yellow, this is a green' assessment. It needs to be a 'this is a $65 million risk that can be addressed with $3 million investment and the right tools'.*
>
> **Corey Hamilton, IBM**

Leading financial institutions have established a cybersecurity resilience plan, reduced ambiguity in terms of responsibility, and fostered a security-first mindset across their organisation. Proper management of existing employees is also critical. Among high-risk and high-level staff, the level of security training remains inconsistent. Less than half of IT leaders were confident in their ability to provide additional cybersecurity training, while about half believe they should deploy further training in general.[11]

The definition of a positive security culture is perhaps the greatest challenge facing financial institutions. While the budget on new systems, solutions, and infrastructure may be towering, understanding the holistic view does not come easy, with 65% of financial services security leaders offering separate definitions for the term "security culture".[12]

> *It is very difficult to measure the forward momentum without the assistance of assurance activities, which may or may not have a technology base. However, rapid development and security of new technologies and their use within the financial space will continue to be a challenge.*
>
> *New technologies such as blockchain and cryptocurrency, plus rapid growth, and now a fully remote work environment expands these problems currently. Rapid implementation can create gaps.*
>
> **Jon Brandt, ISACA**
> **ISACA's 2021 Information Security Advisory Group**

[10] https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/finance/FSI_cyber.pdf

[11] https://ceo.digital/wp-content/uploads/CEO.digital-Dell-report-A03.pdf

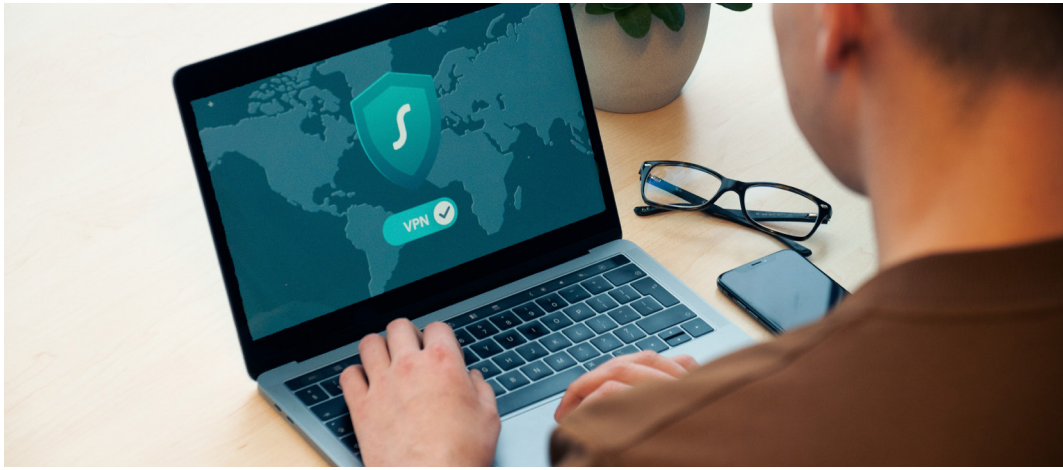
[12] https://www.globalbankingandfinance.com/the-psychology-behind-a-strong-security-culture-in-the-financial-sector/amp

## Conclusions

The challenges brought about by 18 months of upheaval have rocked almost every area of the financial services sector and changed the way we operate forever. That change must be mirrored in the security position of market participants, lest they lose the initiative and fall behind both the bad guys and faster-moving competitors.

A drive to digital has created a forest of new threats, but a few diamonds can be found in the rough in the forms of behavioural data, increased customer centricity, and the deployment of new technology to capitalise on the benefits these can bring. Financial institutions need to ensure that their technology strategy doesn't revolve around simply installing the latest piece of kit and calling it a day, and develop a holistic defence in depth across multiple verticals.

Perhaps most important as we march deeper into the decade and face up to the challenges of a rapidly digital world, is a focus on recruiting, maintaining, and fostering a security culture centred on the people, not the process. Cybersecurity, once simply a subject under which a bank pumped a portion of its budget, has evolved to touch every key structure within the business. Ensuring security is at the forefront of every stakeholder's mind – through training, education, and the deployment of the right processes – should become the core of a bank's future plans.




## About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise, and learning in technology. ISACA equips individuals with knowledge, credentials, education, and community to progress their careers and transform their organisations. It enables enterprises to train and build quality teams that effectively drive IT audit, risk management, and security priorities forward.

ISACA is a global professional association and learning organisation that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk, and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

## About FinTech Futures

*FinTech Futures* is the trusted digital publishing platform for the worldwide fintech community – providing daily news, in-depth analysis, and expert commentary to industry veterans across a comprehensive range of areas.

Our solid reputation, combined with in-depth coverage across global fintech, makes us the leading resource for technology buyers, sellers, developers, integrators, and other specialists across the sector.

With an active presence across key B2B social media platforms including over 50,000 followers on both our Twitter and LinkedIn pages, we deliver upwards of 400,000 impressions monthly through social media alone. This combined with over 200,000 monthly page views on our website, makes us the complete platform for connecting with a relevant audience in the fintech space.

As well as this, our daily newsletter is delivered to over 35,000 key decision-makers in the financial services and technology sectors.

Want to stay informed alongside the industry's best? Sign up today and never miss a story.

**About the author:**

**Alex Hamilton** is deputy editor at *FinTech Futures*. He has been reporting on the financial technology sector for more than five years across a variety of industry publications and has written extensively on digital transformation, cybersecurity, and enterprise technology. He holds a masters degree in ancient history from the University of Nottingham.

He can be contacted at: alex.hamilton@fintechfutures.com



# Reports & Surveys

Sponsorship opportunities are available for our surveys and well-researched topic-specific reports.


## To reach new prospects, talk to:

**Jon Robson**
**Head of Sales**
Email: jon.robson@fintechfutures.com
Tel: +44 208 052 0423

**Sam Hutton**
**Business Development Executive**
Email: sam.hutton@fintechfutures.com
Tel: +44 208 052 0434

Visit **www.fintechfutures.com** for a full list of our reports in 2021